PRESS RELEASE

FICA in the era of deepfake and AI-driven fraud

By Sameer Kumandan, MD of SearchWorks

AI-powered scams are rapidly reshaping the fraud landscape, exposing new vulnerabilities within financial systems and eroding public trust in digital communication. In recent months, there has been a notable increase in cyberattacks that exploit AI to deceive individuals, often by imitating real people with alarming accuracy.

A key strategy involves leveraging AI to produce highly convincing fake images, videos, and audio, commonly referred to as "deepfakes". These are used to impersonate real individuals and spread misleading or false information. While early examples of deepfakes were often unconvincing, recent advancements have made them increasingly difficult to detect, making it easier for bad actors to mislead, manipulate, and defraud.

Momentum Group's Financial Director, Risto Ketola, recently disclosed that he had been impersonated on WhatsApp. Cybercriminals used his LinkedIn profile photo to create a closed WhatsApp group, falsely presenting themselves as Ketola. While this incident did not involve AI-generated imagery or video, it highlights the significant harm that can result when an individual's likeness is misused for malicious purposes.

Deepfake-driven cybercrime has escalated to the point where the South African Banking Risk Information Centre (SABRIC) recently issued a strong warning about the growing threat of AI-enabled fraud. SABRIC specifically highlighted the use of deepfakes and voice cloning to impersonate bank officials, promote fake investment schemes, and fabricate endorsements from well-known public figures. This emerging threat not only compromises the integrity of the financial sector but also erodes customer trust and confidence in digital interactions.

In practice, fraudsters are increasingly using AI to bypass security measures such as automated onboarding systems and Know Your Customer (KYC) checks, enabling them to create accounts and access services under false identities. From a business email compromise (BEC) standpoint, attackers are now incorporating deepfake audio and video of senior executives into phishing attempts, convincing employees to release funds or disclose sensitive information. Social engineering attacks have also become more sophisticated, with AI being used to analyse and replicate communication styles based

on publicly available information, making scams appear more authentic. In some cases, AI is used to generate entirely synthetic identities, combining real and fabricated data to create fake personas capable of applying for credit, laundering money, or committing large-scale financial fraud. Unfortunately, many legacy fraud detection tools aren't designed to detect fake audio or video, making deepfake scams harder to spot.

In response, financial institutions must urgently evolve their fraud prevention strategies to stay ahead of sophisticated threats. Regulators expect financial institutions to keep up with the latest cybercrime trends and failing to detect deepfake-based fraud can result in compliance failures, fines, and legal action. Furthermore, financial institutions must consider the broader impact of these risks on customer trust. As awareness of deepfake threats grows, it is understandable that clients may begin to question the authenticity of video calls, digital signatures, and other remote interactions. This erosion of confidence has the potential to hinder digital transformation initiatives and may even prompt some customers to disengage from digital platforms altogether.

VOCA, powered by SearchWorks, provides financial institutions with the verified data and intelligent processes needed to limit exposure to fraud and ensure regulatory compliance. By leveraging real-time data and automated checks, VOCA helps organisations verify the identity and legitimacy of individuals and entities they engage with. It flags discrepancies, detects suspicious behaviour, and highlights incomplete or false information, supporting informed decision-making at every stage. Through continuous monitoring of client behaviour and borrower risk profiles, VOCA enables early identification of potential threats, helping institutions close compliance gaps, avoid financial penalties, and stay ahead of emerging fraud risks.

Ends.